Guide For Using Onion Browser On iOS

INFO :

Onion Browser is a free and open-source web browser for iPhone and iPad that encrypts and tunnels web traffic through the Tor network, with extra features to help you browse the internet privately , it's not developed by tor project but they advised iOS users to use it also we advice to use it as secure alternative for Safari which is developed by Apple

مؤسسة آفاق الإلكترونية
تهتم بنشر الوعي الأمني
والتقني بين المسلمين

بسم الله الرحمن الرحيم

Onion Browser is a free and open-source web browser for iPhone and iPad that encrypts and tunnels web traffic through the Tor network, with extra features to help you browse the internet privately , it’s not developed by tor project but they advised iOS users to use it also we advice to use it as secure alternative for Safari which is developed by Apple

Browser Features :

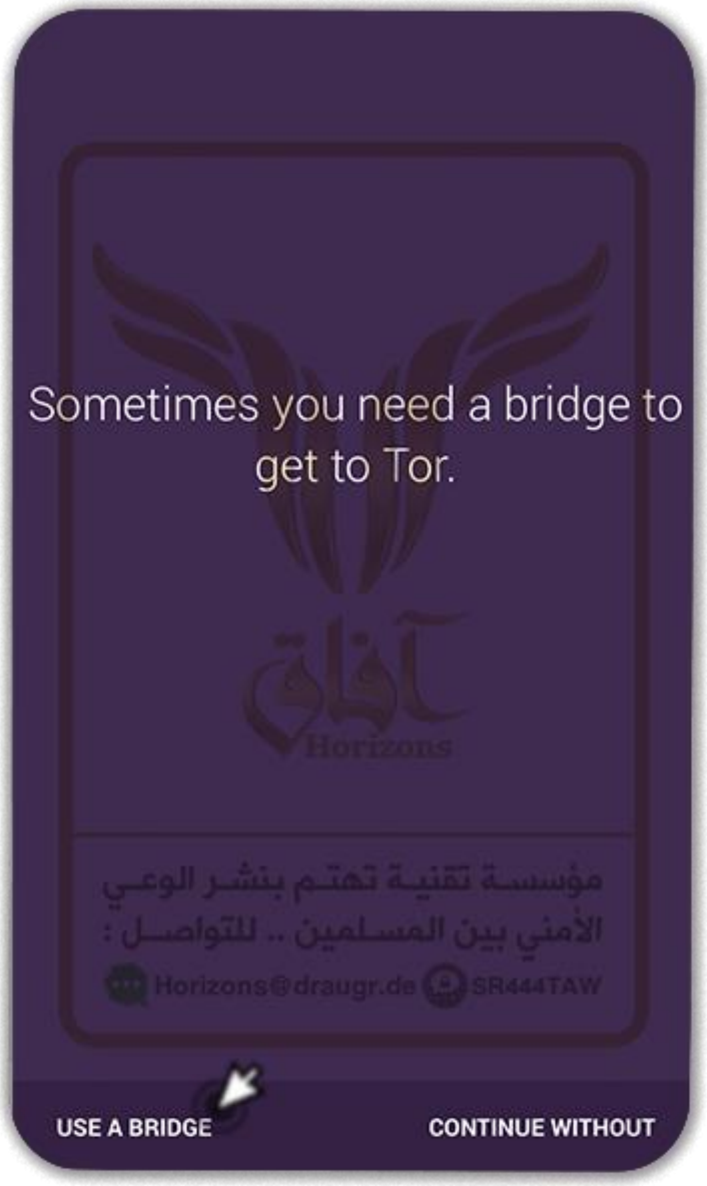
- Internet access is tunneled through the Tor network[1][2]
    - Websites do not see your real IP address.
    - ISPs and insecure wireless networks cannot see your browsing.
    - Access websites, even behind some types of internet filters and censors.
    - View .onion websites: the “dark net” of hidden sites only accessible using Tor.
- Block third party cookies or all cookies.
- Ability to change cookie storage policy (Allow All / Block Third Party / Block All)
- Disable scripts and multimedia content that can be used to track you.
- Can send the “Do Not Track” HTTP header (DNT: 1) to websites.

Security Notes :

- Onion Browser only tunnels traffic *within the Onion Browser app*. You are still using a smartphone you should be aware that information outside of Onion Browser will continue to use your normal connection
- iOS has full control over some network traffic, which may result in this traffic (including audio or video embeds) routing via your normal connection and not over Tor
- Websites may use Javascript to ask the browser for local time, therefore revealing your real time zone. Disabling Javascript (using the Strict security setting) is the only way to bypass this
- Websites may use the HTML5 Geolocation API (to view your current GPS location) and other new HTML5 features unless “Strict” security mode is set. Users should also remain vigilant for any pop-ups asking for permission to access location data.
- If you log into websites in Onion Browser that you normally log into outside of the Tor network, they will or still know who you are, and know that you use Tor. In certain circumstances (i.e. political dissent in repressive nations), this may be incriminating information in itself.

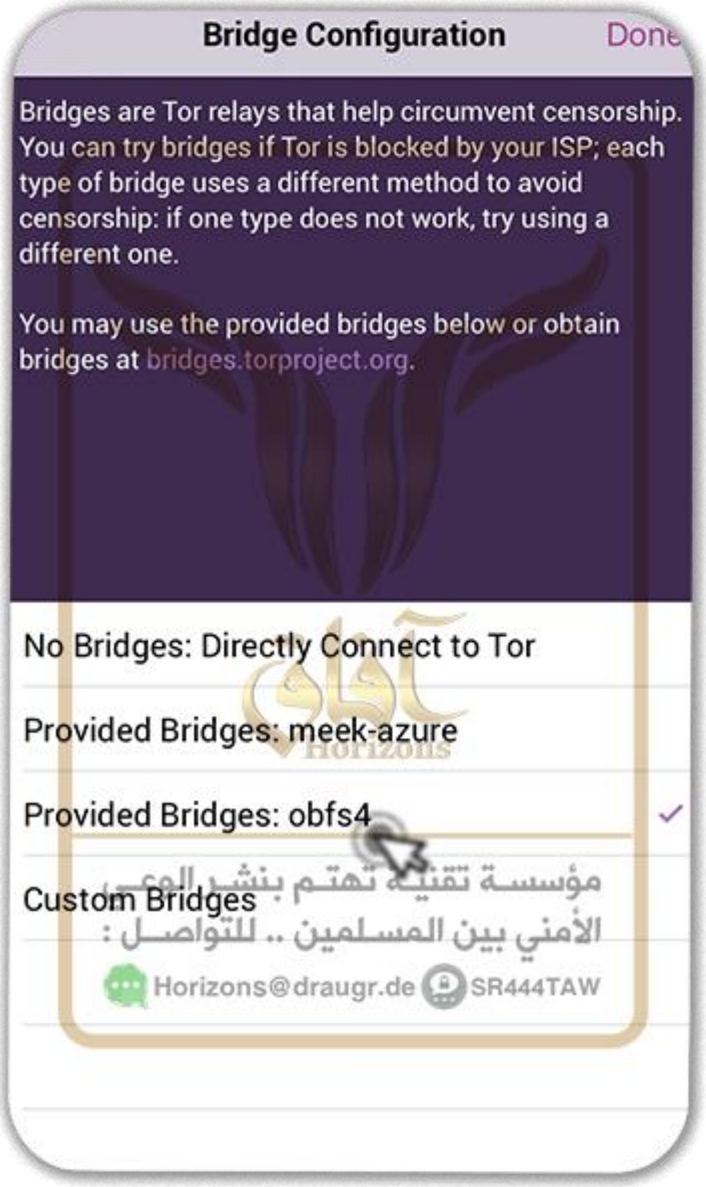
How To Use :

- Press on use ” USE A BRIDGE “



Sometimes you need a bridge to get to Tor.

- Press on ” Obfs4”



Bridge Configuration

Done

Bridges are Tor relays that help circumvent censorship. You can try bridges if Tor is blocked by your ISP; each type of bridge uses a different method to avoid censorship: if one type does not work, try using a different one.

You may use the provided bridges below or obtain bridges at bridges.torproject.org.

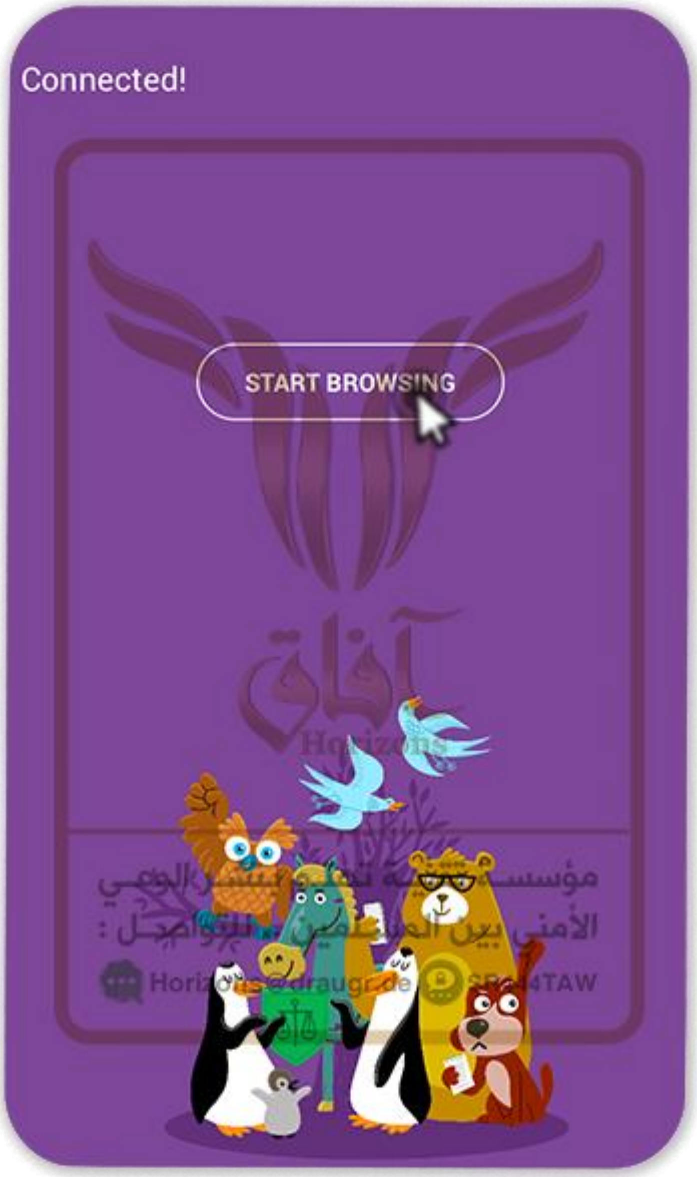
No Bridges: Directly Connect to Tor

Provided Bridges: meek-azure

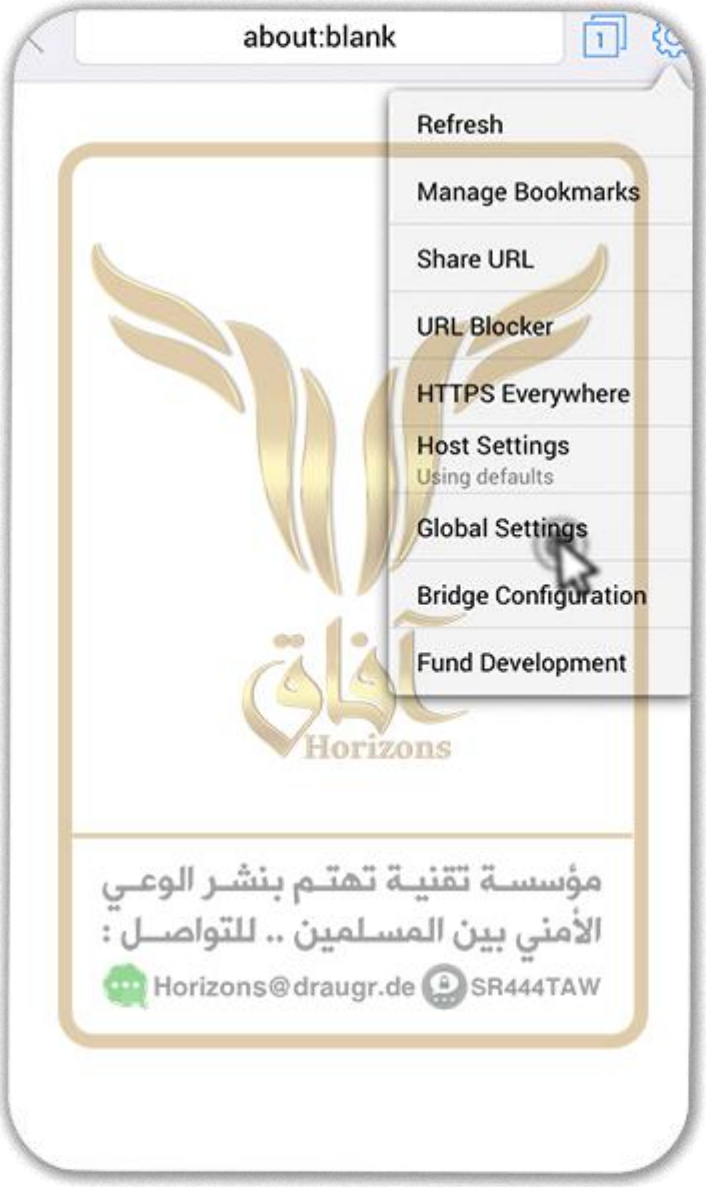
Provided Bridges: obfs4 ✓

Custom Bridges

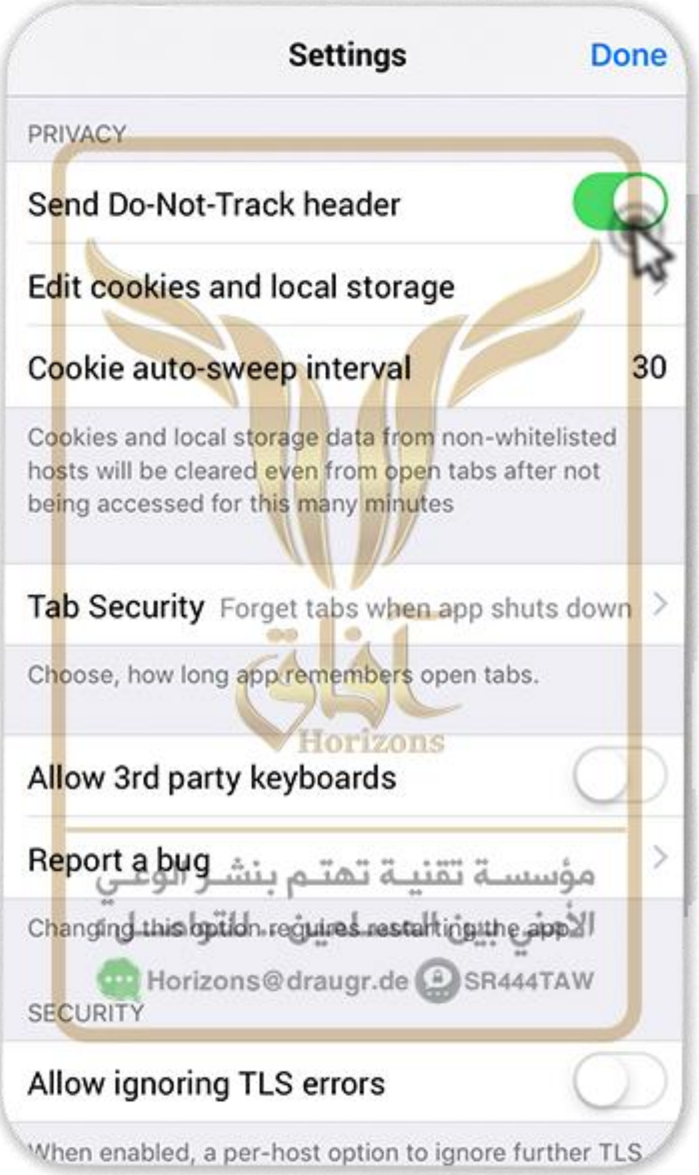
- Press on Start Browsing



- Press on ” Global Settings “



- Press on ” Send Do-Not-Track Header ”



Settings Done

PRIVACY

Send Do-Not-Track header

Edit cookies and local storage

Cookie auto-sweep interval 30

Cookies and local storage data from non-whitelisted hosts will be cleared even from open tabs after not being accessed for this many minutes

Tab Security Forget tabs when app shuts down

Choose, how long app remembers open tabs.

Allow 3rd party keyboards

Report a bug

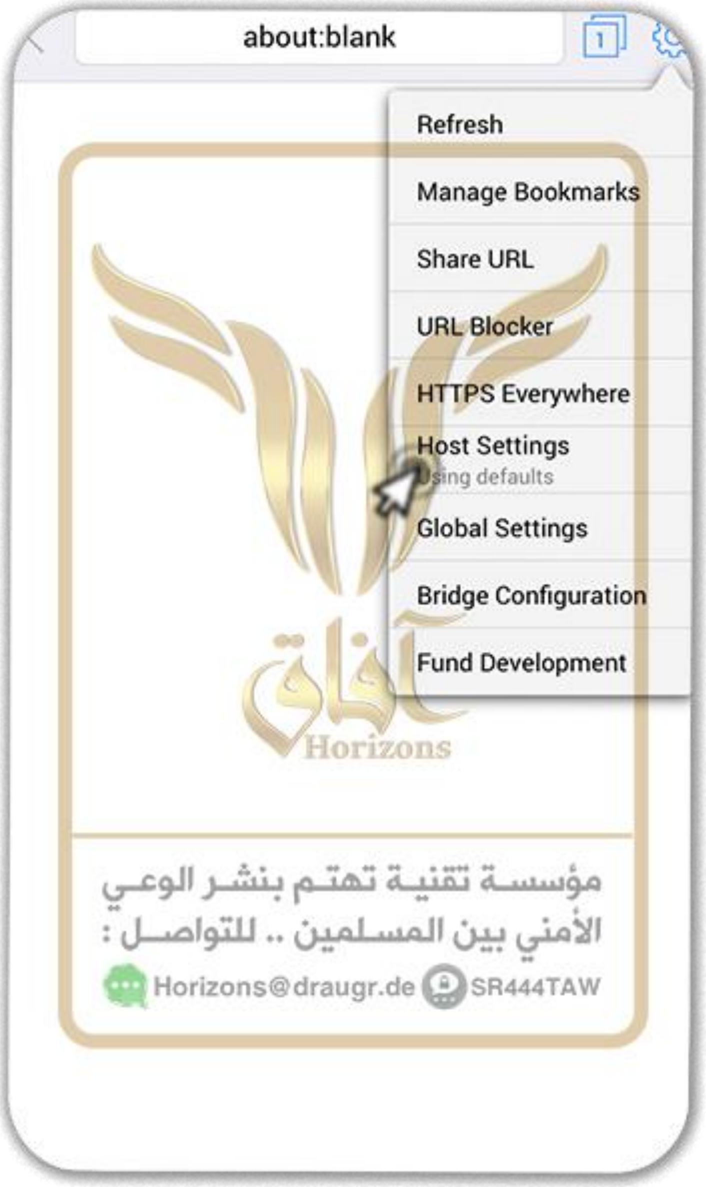
Changing this option requires restarting the app.

SECURITY

Allow ignoring TLS errors

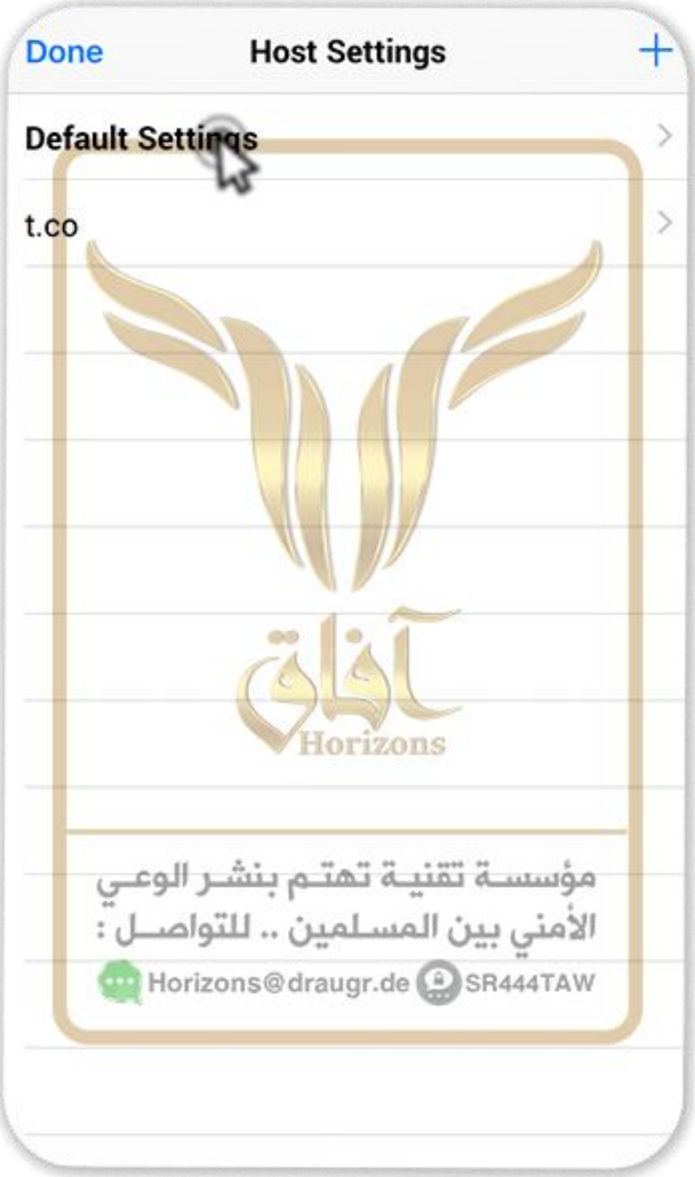
When enabled, a per-host option to ignore further TLS

- Go back to the app menu and press on ” Host Settings “

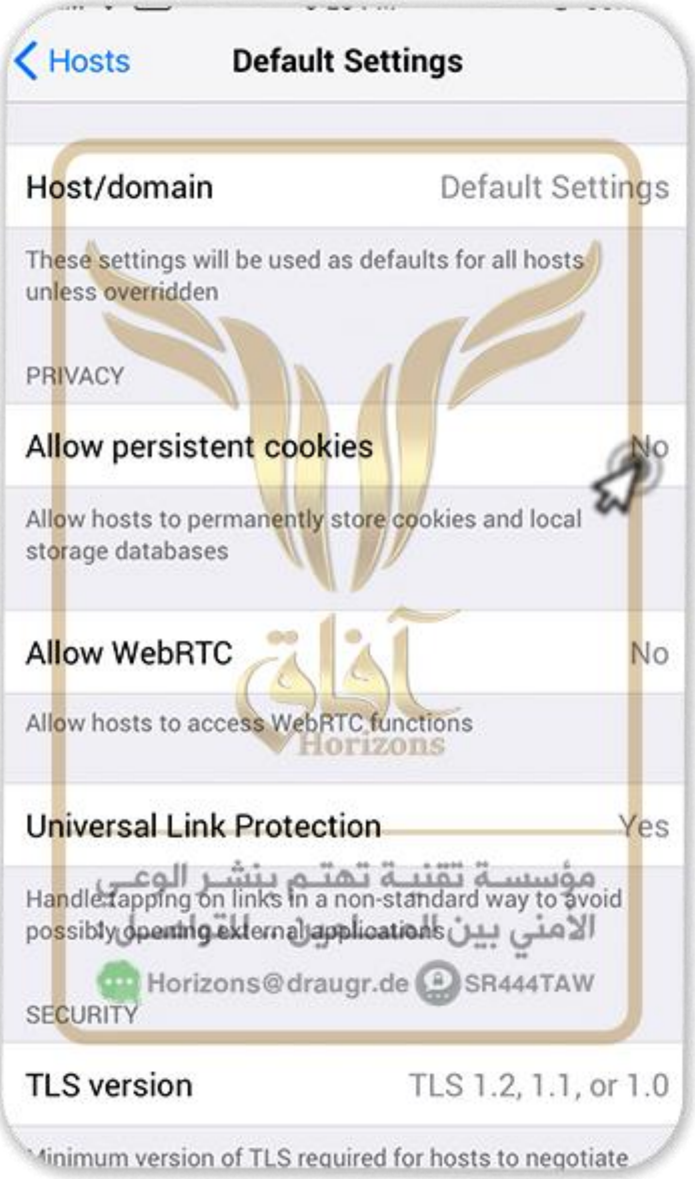


about:blank

- Press on “Default Settings “



- Press on ” Allow Persistent Cookies” and choose No ” press on ” Allow WebRTC ” and choose “No “



Hosts Default Settings

Host/domain Default Settings

These settings will be used as defaults for all hosts unless overridden

PRIVACY

Allow persistent cookies No

Allow hosts to permanently store cookies and local storage databases

Allow WebRTC No

Allow hosts to access WebRTC functions

Universal Link Protection Yes

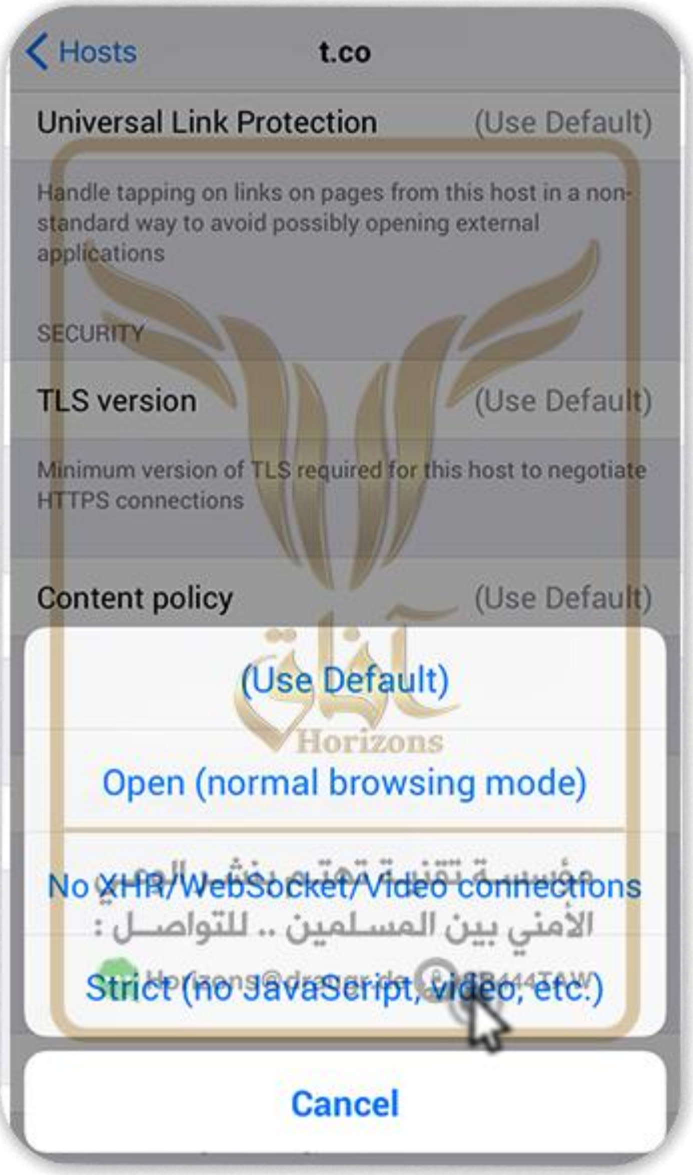
Handle tapping on links in a non-standard way to avoid possibly opening external applications

SECURITY

TLS version TLS 1.2, 1.1, or 1.0

Minimum version of TLS required for hosts to negotiate

- Select " Content policy



Hosts

t.co

Universal Link Protection (Use Default)

Handle tapping on links on pages from this host in a non-standard way to avoid possibly opening external applications

SECURITY

TLS version (Use Default)

Minimum version of TLS required for this host to negotiate HTTPS connections

Content policy (Use Default)

(Use Default)

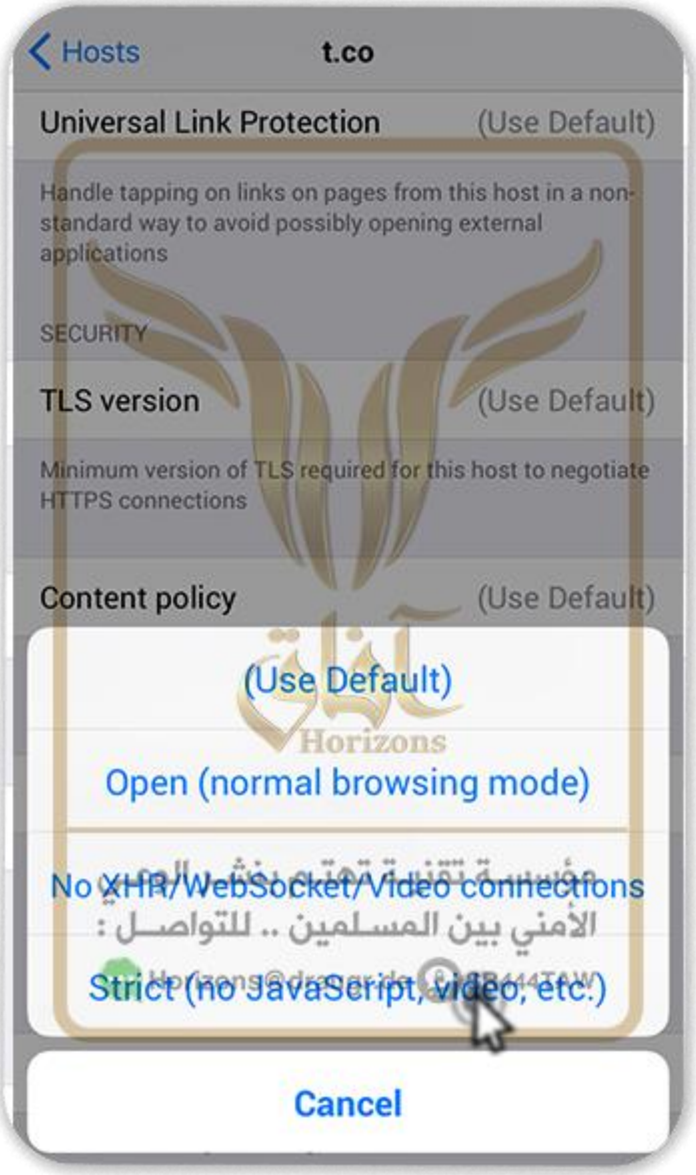
Open (normal browsing mode)

No XHR/WebSocket/Video connections

Strict (no JavaScript, video, etc.)

Cancel

- Select " Strict "



Universal Link Protection (Use Default)

Handle tapping on links on pages from this host in a non-standard way to avoid possibly opening external applications

SECURITY

TLS version (Use Default)

Minimum version of TLS required for this host to negotiate HTTPS connections

Content policy (Use Default)

(Use Default)
Open (normal browsing mode)
No XHR/WebSocket/Video connections
Strict (no JavaScript, video, etc.)
Cancel

آفاق
Horizons

مؤسسة آفاق الإلكترونية

SR444TAW

Horizons@draugr.de